Realization of Quantum State Privacy Amplification in a Nuclear Magnetic Resonance Quantum System*

Liang Hao[1], Chuan Wang[1,2] and Gui Lu Long[1,3]
[1] *Key Laboratory for Atomic and Molecular NanoSciences and Department of Physics, Tsinghua University, Beijing 100084, P. R. China*
[2] *School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[3] *Tsinghua National Laboratory for Information Science and Technology, Beijing 100084, China*

Quantum state privacy amplification (QSPA) is the quantum analogue of classical privacy amplification. If the state information of a series of single particle states has some leakage, QSPA reduces this leakage by condensing the state information of two particles into the state of one particle. Recursive applications of the operations will eliminate the quantum state information leakage to a required minimum level. In this paper, we report the experimental implementation of a quantum state privacy amplification protocol in a nuclear magnetic resonance system. The density matrices of the states are constructed in the experiment, and the experimental results agree with theory well.

PACS numbers: 03.67.Dd, 03.67.Hk,03.67.Ac
Keywords: quantum state privacy amplification, QSPA, nuclear magnetic resonance, quantum secure direct communication

I. INTRODUCTION

The combination of quantum physics with communication gives rise to quantum communication. The physics principles of quantum mechanics offer the advantage of provable security, and higher capacity of quantum communication over its classical counterparts. There are various quantum communication tasks, such as quantum key distribution where random keys are distributed among two users separated at a distance [1–4], quantum secret sharing [5–10] where a secret is shared among several users and the users can read out the shared secret only by cooperation, and quantum secure direct communication [11–17] where secret messages are transmitted directly over a quantum channel. They serve the various needs of communication.

Under practical conditions, quantum communication is inevitably affected by noise in quantum channels. It is hard to distinguish whether the errors are due to an eavesdropping behavior or the noise in the channel itself. Therefore quantum communication over a noisy channel is not completely secure, and some post-processing must be done. For instance in quantum key distribution, privacy amplification [20] is performed to distill secure keys from the less secure raw keys. Quantum privacy amplification [21–23] is exploited for a sequence of entangled Einstein-Podolsky-Rosen (EPR) pairs so as to obtain maximally entangled pairs in protocols using EPR pairs.

In some quantum communication protocols, in the end and intermediate results of the quantum communication, there are a sequence of single photons in nonorthogonal quantum states [15, 18, 19], for instance in states $|0\rangle$, $|1\rangle$, $|+x\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-x\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, where $|0\rangle$ and $|1\rangle$ represent the horizontal and vertical polarization state of the photon respectively. These single photons are sent from Bob to Alice. After eavesdropping check, Alice encodes the bit values on the single photons by performing some unitary operations, and then sends the encoded photons back to Bob. If the information of the quantum states of the photons are leaked due to either eavesdropping or channel noise, then one needs to reduce the information leakage by some operation. The usual privacy amplification used in QKD post-processing is not applicable, because the single photons are in states in two conjugate basis, and they cannot be added together in the manner used for the usual privacy amplification. Quantum privacy amplification designed for the EPR based protocols is not applicable to this case either, because the single photons are not entangled states. For this purpose, quantum state privacy amplification was proposed recently [24] and it reduces the information leakage in the quantum states of single photons. The essential idea of QSPA [24] is to perform combined operations of controlled-NOT gates and Hadamard gates on two qubits, and make a measurement on one qubit. Using the measurement result, one can specify the state of the remaining qubit. However the state of remaining particle is unknown to an adversary, hence reduces his/her knowledge of the quantum state. In this way, the information leakage is reduced.

It is appealing to choose the nuclear magnetic resonance (NMR) system to implement the QSPA protocol. First,

* Liang Hao, ChuanWang and Gui Lu Long, J. Phys. B: At. Mol. Opt. Phys. 43 (2010) 125502 (6pp), doi:10.1088/0953-4075/43/12/125502

the NMR technique is a well-developed and sophisticated technique. It has been a powerful tool for experimental study of quantum information processing which can demonstrate the quantum manipulation of various quantum information processing tasks. The essential features of quantum algorithms can be demonstrated in such a quantum system, and the technique developed in NMR system is also helpful in other candidate quantum systems. For example, many quantum algorithms have been successfully demonstrated in NMR quantum system [25–30], and some quantum communication protocols, such as teleportation [31] and dense coding [32, 33], have been implemented in the NMR system. Secondly, quantum gates are relatively easier to implement in NMR system than in optical system. For transmission, it is no doubt that optical system is the best candidate information carrier. However in terms of gate operations, NMR system is easier because the quantum gates can be realized by radio-frequency pulses and free evolutions. Thus, demonstrating quantum algorithms in NMR enjoys the ease of gate operations while testing the essential quantum operations. On the other hand, there have been many efforts in building interfaces between flying qubits and stationary qubits [34–37]. The combination of flying qubits and stationary qubits may be a good candidate for quantum information processing, especially for those involving both the transmission and processing of qubits. If such interface could be successfully build, nuclear spin qubit may well be a good candidate of stationary qubit. In that case, the flying photon qubit may first be transferred to a stationary electron spin qubit, and then further transferred to nuclear spin qubit.

This paper reports the experimental study of QSPA in a nuclear magnetic resonance quantum system. In this work, we have experimentally implemented the QSPA protocol in a nuclear magnetic resonance system, and all the quantum operations needed in the QSPA are demonstrated. Density matrices of states during the QSPA were constructed. The experimental results agree with theory well.

II. THE PRINCIPLE OF QUANTUM STATE PRIVACY AMPLIFICATION

Firstly, we briefly describe the QSPA protocol, for details see Ref. [24]. It is the quantum analogue of classical privacy amplification. In classical cryptography, if a sequence key of n bits has some leakage to the outside, the legitimate users can use the privacy amplification to reduce this information leakage. The common privacy amplification protocol [20] uses the parities of m partitions of subsets of the original raw key with some permutations. Thus, instead of using the original n-bits key, the legitimate users use m bits of parities as the new key. Usually, m is less than n, the privacy of the key has been amplified, and hence has better security. The task of QSPA is as follows. Two single-qubit states,

$$\begin{aligned} |\varphi\rangle_1 &= a_1|0\rangle + b_1|1\rangle, &(1)\\ |\varphi\rangle_2 &= a_2|0\rangle + b_2|1\rangle, &(2)\end{aligned}$$

where the coefficients a_1, b_1, a_2 and b_2 satisfy the normalization requirement,

$$|a_1|^2 + |b_1|^2 = |a_2|^2 + |b_2|^2 = 1, \tag{3}$$

are known to the legitimate users, and however have an information leakage to an adversary Eve. The task of QSPA is to reduce this state information leakage. Because the single-qubit states are usually not orthogonal, the approach to take the parity is not applicable. Instead, the quantum state privacy amplification protocol in Ref.[24] uses two controlled-not (CNOT) gates and a Hadamard (H) gate, which may be simply called the CHC operation (for simplicity, we call this QSPA protocol as CHC-QSPA protocol hereafter). The schematic circuit is shown in Fig.1. The initial state $|\psi\rangle_{in}$ of the QSPA is the product of two single photon states,

$$|\psi\rangle_{in} = |\varphi\rangle_1 \otimes |\varphi\rangle_2 . \tag{4}$$

After the CHC operation, the state of the joint system is changed to

$$\begin{aligned} |\psi\rangle_{out} = &\frac{1}{\sqrt{2}}\{(a_1a_2 + b_1b_2)|0\rangle_1 + (a_1b_2 - b_1a_2)|1\rangle_1\}|0\rangle_2 \\ &+\frac{1}{\sqrt{2}}\{(a_1a_2 - b_1b_2)|1\rangle_1 + (a_1b_2 + b_1a_2)|0\rangle_1\}|1\rangle_2 . \end{aligned} \tag{5}$$

Then one measures the second qubit in the σ_z basis. If $|\varphi\rangle_{2,out} = |0\rangle$ is obtained, the state of control qubit is

$$|\varphi\rangle_{1,out} = (a_1a_2 + b_1b_2)|0\rangle_1 + (a_1b_2 - b_1a_2)|1\rangle_1 . \tag{6}$$

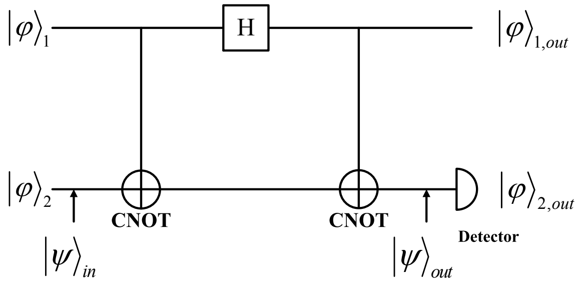


FIG. 1: Circuit of the CHC-QSPA protocol. $|\varphi_1\rangle$ and $|\varphi_2\rangle$ denotes the states of the two qubits, respectively. The target qubit is measured at the end so as to incorporate the state information of the second qubit into the first qubit.

Otherwise, the first qubit state is

$$|\varphi\rangle_{1,out} = (a_1a_2 - b_1b_2)\,|1\rangle_1 + (a_1b_2 + b_1a_2)\,|0\rangle_1\,. \tag{7}$$

In this way, no matter what the measurement result of second qubit is, the state information of two qubits is concentrated on the first one. So the privacy of the state is amplified.

	φ_1			
φ_2	$\vert +z\rangle$	$\vert -z\rangle$	$\vert +x\rangle$	$\vert -x\rangle$
$\vert +z\rangle$	$\vert 0\rangle$	$\vert 1\rangle$	$\vert -x\rangle$	$\vert +x\rangle$
$\vert -z\rangle$	$\vert 1\rangle$	$\vert 0\rangle$	$\vert +x\rangle$	$\vert -x\rangle$
$\vert +x\rangle$	$\vert +x\rangle$	$\vert -x\rangle$	$\vert 0\rangle$	$\vert 1\rangle$
$\vert -x\rangle$	$\vert -x\rangle$	$\vert +x\rangle$	$\vert 1\rangle$	$\vert 0\rangle$

TABLE I: The truth table of the output state for the control qubit $|\varphi\rangle_{1,out}$, when the measurement result of the target qubit is $|0\rangle$. $|\varphi\rangle_1$ and $|\varphi\rangle_2$ are the input states of the control and target qubit,respectively.

	φ_1			
φ_2	$\vert +z\rangle$	$\vert -z\rangle$	$\vert +x\rangle$	$\vert -x\rangle$
$\vert +z\rangle$	$\vert 1\rangle$	$\vert 0\rangle$	$\vert +x\rangle$	$\vert -x\rangle$
$\vert -z\rangle$	$\vert 0\rangle$	$\vert 1\rangle$	$\vert -x\rangle$	$\vert +x\rangle$
$\vert +x\rangle$	$\vert +x\rangle$	$\vert -x\rangle$	$\vert 0\rangle$	$\vert 1\rangle$
$\vert -x\rangle$	$\vert -x\rangle$	$\vert +x\rangle$	$\vert 1\rangle$	$\vert 0\rangle$

TABLE II: The truth table of the output state of the control qubit $|\varphi\rangle_{1,out}$, when the measurement result of the target qubit is $|1\rangle$. $|\varphi\rangle_1$ and $|\varphi\rangle_2$ are the input states of the control and target qubit,respectively.

We take the quantum one-time-pad protocol [15] as an example, where the single photon states are $|\pm x\rangle$ and $|\pm z\rangle$ respectively. The truth table of the output state of first qubit $|\varphi\rangle_{1,out}$ is shown in Tables I and II for the measurement results of the target qubit $|0\rangle$ and $|1\rangle$, respectively. When $|\varphi\rangle_1 = |0\rangle$, $|\varphi\rangle_2 = |1\rangle$, after the CHC operation, the output state is

$$|\psi\rangle_{out} = \frac{1}{\sqrt{2}}(|1\rangle_1\,|0\rangle_2 + |0\rangle_1\,|1\rangle_2). \tag{8}$$

If the measurement result of the target qubit $|\varphi\rangle_{2,out} = |0\rangle$, the final state of the control qubit $|\varphi\rangle_{1,out} = |1\rangle$. So the privacy of the input state $|0\rangle_1\,|1\rangle_2$ is concentrated on the final state of the control qubit $|1\rangle_1$. If $|\varphi\rangle_{2,out} = |1\rangle$ is obtained, the initial key $|0\rangle_1\,|1\rangle_2$ is compressed to the condensed key $|0\rangle_1$. It is obvious that the condensed key depends not only on the input states of two single photons, but also on the result of the measurement on the target qubit.

Suppose an adversary Eve knows the complete information of the control qubit but nothing about the target qubit. She can only guess the input state of the target qubit to deduce the condensed key. In most quantum communication protocols, the single photons prepared by the legitimate user are in one of the four states $|0\rangle$, $|1\rangle$, $|+x\rangle$, $|-x\rangle$ randomly. Even if Eve knows completely the information of both qubits, which is a small probability event[24], she can not deduce the condensed state with certainty, because the final state of the control qubit $|\varphi\rangle_{1,out}$ has two possible results even though the input state $|\psi\rangle_{in}$ is fixed. The output state depends on the measurement result of the target qubit, according to the truth tables, when the input state $|\varphi\rangle_2 = |0\rangle$.

In practice, the process of QSPA can be used repeatedly to get more secure quantum state by using the retained qubit from the last round as a control and choosing a third qubit from the sequence as the target. The more one repeats the QSPA operations, the lower the state information leakage.

III. NMR REALIZATION

The QSPA protocol was experimentally realized in NMR in a sample of Carbon-13 labeled chloroform (^{13}CHCL$_3$) which was dissolved in d6 acetone. The experiments were done at $22°C$ with a Bruker Avance III 400 MHz spectrometer. We assign the ^{13}C as the control qubit, and the ^{1}H as the target qubit, here the two qubits are denoted as C1 and H2. With the convention that magnetic field is along the z-axis, we define the spin up $|\uparrow\rangle$ as $|0\rangle$ state and spin down $|\downarrow\rangle$ as $|1\rangle$ state, which correspond to the low-frequency part and high-frequency part of the spectrum respectively. The system Hamiltonian is

$$H_{NMR} = -\pi\nu_1\sigma_z^1 - \pi\nu_2\sigma_z^2 + \frac{1}{2}\pi J_{12}\sigma_z^1\sigma_z^2, \tag{9}$$

where ν_1 and ν_2 are the resonance frequencies for C1 and H2, respectively. The scalar coupling between two spins J_{12} has been measured to be 215Hz.

The pseudopure state $|0\rangle_1 |0\rangle_2$ is prepared from the thermal equilibrium state of the two qubits system using the spatial averaging method [26, 29], where the pulse sequence is $[\theta]_x^2 \rightarrow [grad]_z \rightarrow [-\pi/4]_x^2 \rightarrow [1/2J] \rightarrow [\pi/4]_y^2 \rightarrow [grad]_z$, where $[grad]_z$ is the gradient field. The state evolution under these pulses is

$$\begin{array}{rl}
 & \gamma_C I_z^1 + \gamma_H I_z^2 \\
[\theta]_x^2 \Rightarrow & \gamma_C(I_z^1 + 2I_z^2) - \sqrt{1 - \frac{4\gamma_C^2}{\gamma_H^2}} I_y^2 \\
[grad] \Rightarrow & \gamma_C(I_z^1 + 2I_z^2) \\
\left[\frac{\pi}{4}\right]_{-x}^2 \Rightarrow & \gamma_C(I_z^1 + \sqrt{2}I_z^2 + \sqrt{2}I_y^2) \\
\left[\frac{1}{2J_{12}}\right] \Rightarrow & \gamma_C(I_z^1 + \sqrt{2}I_z^2 - 2\sqrt{2}I_z^1 I_x^2) \\
\left[\frac{\pi}{4}\right]_y^2 \Rightarrow & \gamma_C(I_z^1 + I_z^2 + I_x^2 - 2I_z^1 I_x^2 + 2I_z^1 I_z^2) \\
[grad] \Rightarrow & 2\gamma_C[(\frac{1}{2} + I_z^1)(\frac{1}{2} + I_z^2) - \frac{1}{4}],
\end{array} \tag{10}$$

where $[\theta]_\alpha^k$ is defined as the rotation of spin k through angle θ about $\hat{\alpha}$-axis. $[\tau]$ is the free evolution of the system for τ time interval, and $[grad]_z$ denotes a gradient pulse along the $\hat{z}$-axis. Accordingly,

$$\cos\theta = 2\gamma_C/\gamma_H, \tag{11}$$

where γ_C and γ_H are the gyromagnetic ratios of spin ^{13}C and proton ^{1}H, respectively.

The pulse sequence of the QSPA operation in the CHC-QSPA protocol is found to be

$$\begin{array}{l}
[\frac{\pi}{2}]_y^2 \rightarrow [\frac{1}{2J_{12}}] \rightarrow [\pi]_{-y}^2 \rightarrow [\frac{\pi}{2}]_x^2 \\
\rightarrow [\frac{\pi}{2}]_z^{1,2} \rightarrow [\frac{\pi}{2}]_y^1 \rightarrow [\pi]_{-x}^1 \rightarrow [\frac{\pi}{2}]_y^2 \\
\rightarrow [\frac{1}{2J_{12}}] \rightarrow [\pi]_{-y}^2 \rightarrow [\frac{\pi}{2}]_x^2 \rightarrow [\frac{\pi}{2}]_z^{1,2}.
\end{array} \tag{12}$$

The optimized CNOT gate pulse sequence is shown in Fig.2. The free evolution $[\frac{1}{2J_{12}}]$ is realized by using a free time delay $\tau = 1/4J_{12}$ separated by a pair of π pulses in the opposite directions, and these pulses can average out the

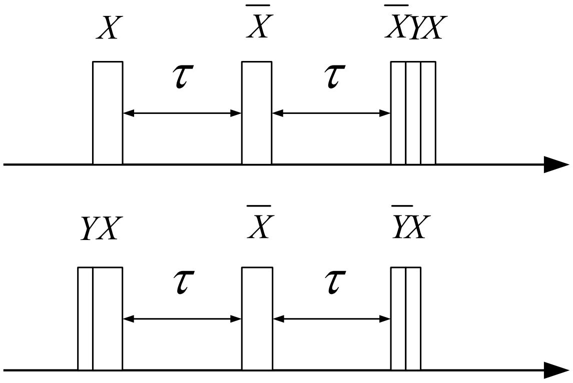


FIG. 2: Optimal NMR pulse sequence for the controlled-NOT gate. The wide and narrow boxes denote π and $\pi/2$ pulses, respectively. the upper and lower lines are for the control and target qubits respectively. X and Y denote the axes along which the pulses are applied, and the overbars indicate the opposite direction. The time period τ, during which no pulses are applied, is set equal to $1/4J_{12}$. The order of pulses are from the left to the right.

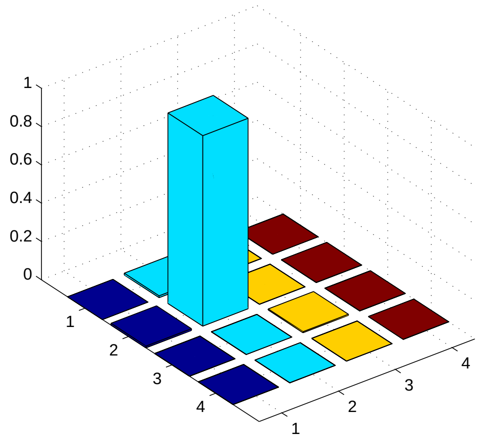
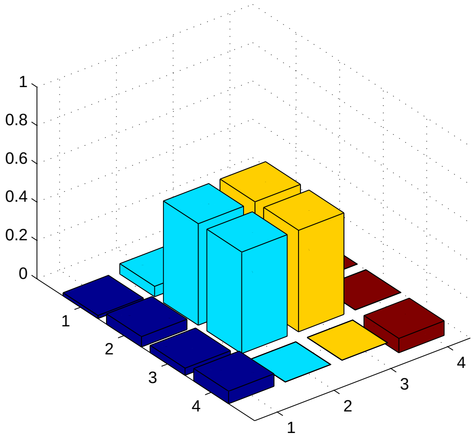


FIG. 3: The density matrix of initial state $|\psi\rangle_{in} = |0\rangle_1 |1\rangle_2$.

effects of free Hamiltonian evolution of two spins σ_z^1 and σ_z^2. In this way, we can also reduce the error accumulations caused by imperfect calibration of the π pulses. The H gate is implemented by a $\pi/2$ pulse along $\hat{y}$-axis, followed by a π pulse along $\hat{-x}$-axis.

We have implemented the QSPA protocol for two kinds of initial states, $|\psi\rangle_{in} = |0\rangle_1 |1\rangle_2$, and $|\psi\rangle_{in} = \left(\frac{\sqrt{3}}{2}|0\rangle_1 + \frac{1}{2}|1\rangle_1\right)(\cos 15^o |0\rangle_2 + \sin 15^o |1\rangle_2)$. The state $|0\rangle_1 |1\rangle_2$ can be obtained by rotating the second spin π about $\hat{y}$-axis from the pseudopure state $|0\rangle_1 |0\rangle_2$. The experimental density matrix for initial state $|0\rangle_1 |1\rangle_2$ is shown in Fig.3. After the CHC-operation, the outcome state is $|\psi\rangle_{out} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, and the experimental density matrix was reconstructed by state tomography technique [38, 39] and is shown in Fig. 4. The density matrices agree with theoretical predictions very well.

For quantum communication, the case with state $|\psi\rangle_{in} = \left(\frac{\sqrt{3}}{2}|0\rangle_1 + \frac{1}{2}|1\rangle_1\right)(\cos 15^o |0\rangle_2 + \sin 15^o |1\rangle_2)$ is more interesting because it represents the more general nonorthogonal state case. The state $\left(\frac{\sqrt{3}}{2}|0\rangle_1 + \frac{1}{2}|1\rangle_1\right)(\cos 15^o |0\rangle_2 + \sin 15^o |1\rangle_2)$ can be prepared by applying $[\frac{2\pi}{3}]_y^1 \rightarrow [\frac{\pi}{3}]_y^2$ to the pseudopure state. The density matrices of the initial and output state are shown in Fig.5 and 6 respectively. For comparisons, we



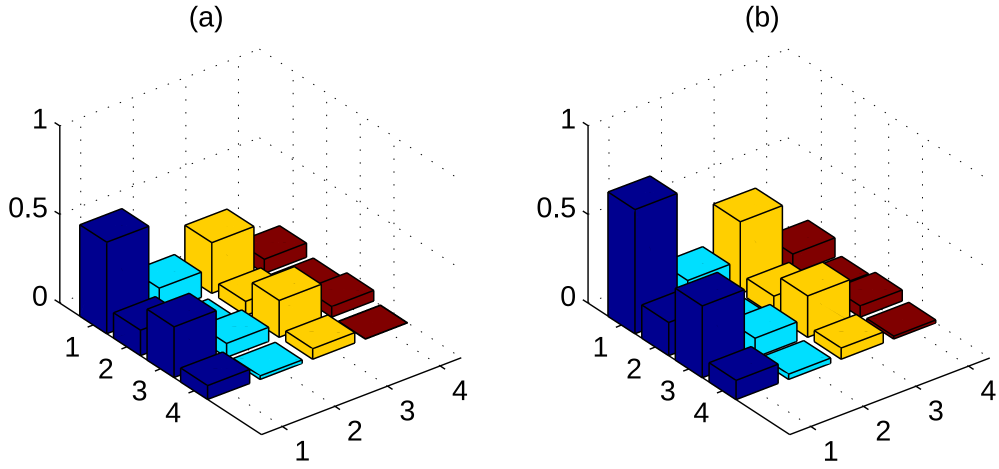


FIG. 5: The density matrix of initial state $|\psi\rangle_{in} = \left(\frac{\sqrt{3}}{2}|0\rangle_1 + \frac{1}{2}|1\rangle_1\right)\left(\cos 15^o |0\rangle_2 + \sin 15^o |1\rangle_2\right)$: (a) experiment result; (b) theoretical prediction.

have also shown the theoretical density matrices for these states. The output state has a more complicated form for this initial state, and it is $|\psi\rangle_{out} = (0.6830\,|00\rangle + 0.5000\,|01\rangle - 0.1830\,|10\rangle + 0.5000\,|11\rangle)$. Fig.6(a) shows the density matrix of the outcome state. The agreement between theory and experiment is good.

IV. SUMMARY

In conclusion, we have constructed the pulse sequence for the QSPA operation in the CHC-QSPA protocol. The results of the experiments agree with the theoretical predictions well both in the case with computational basis states and the general case of nonorthogonal states. The output carries the state information of two qubits in the QSPA. With the information about the measurement result and the information of the two input qubits, a legitimate user knows the state of qubit after QSPA, whereas an illegal user lacks the proper information of all the qubits involved, and hence loses his/her knowledge about the quantum state after the QSPA. In this way, the quantum state information

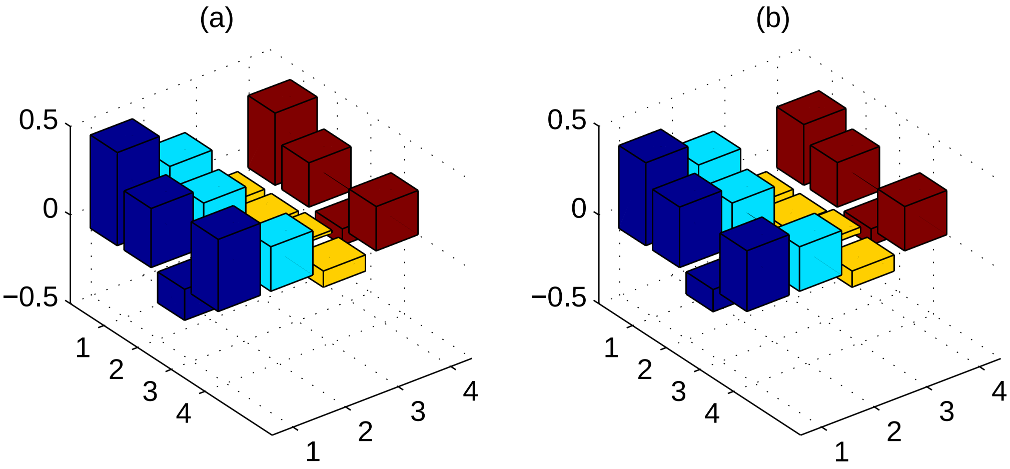


FIG. 6: The density matrix of outcome state after the CHC-operation $\left(\frac{\sqrt{3}}{2}\left|0\right\rangle_1+\frac{1}{2}\left|1\right\rangle_1\right)\left(\cos 15^o\left|0\right\rangle_2+\sin 15^o\left|1\right\rangle_2\right)$: (a) experimental result; and (b) theoretical result.

leakage is reduced. The present experiment clearly demonstrated the protocol.

This work is supported by the National Natural Science Foundation of China Grant No. 10874098, the National Basic Research Program of China (2006CB921106, 2009CB929402).

References

[1] C. H. Bennett, G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing. Bangalore, India, IEEE, New York, 175 (1984).
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74** 145 (2002).
[4] X. L. Zhang, Y. X. Zhang, and K. L. Gao, Commun. Theor. Phys. **43** 627 (2005).
[5] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59** 1829 (1999).
[6] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59** 162 (1999).
[7] S. Bandyopadhyay, Phys. Rev. A **62** 012308 (2000).
[8] R. Cleve, D. Gottesman, and H. K. Lo, Phys. Rev. Lett. **83** 648 (1999).
[9] Y. M. Li, K. S. Zhang, and K. C. Peng, Phys. Lett. A **324** 420 (2004).
[10] F. G. Deng, X. H. Li, C. Y. Li, P. Zhou, and H. Y. Zhou, Phys. Rev. A **72** 044301 (2005).
[11] G.L. Long and X.S. Liu, Phys. Rev. A 65, 032302 (2002).
[12] A. Beige et al., Acta Phys. Pol. A 101, 357 (2002).
[13] K. Boström and T. Felbinger, Phys. Rev. Lett. **89** 187902 (2002).
[14] F. G. Deng, G. L. Long, and X.S. Liu, Phys. Rev. A **68** 042317 (2003).
[15] F.G. Deng and G.L. Long, Phys. Rev. A **69** 052319 (2004).
[16] F. L. Yan and X. Q. Zhang, Eur. Phys. J. B **41** 75 (2004).
[17] C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, and G. L. Long, Phys. Rev. A **71** 044305 (2005).
[18] Z. J. Zhang, Y. Li and Z. X. Man Phys. Rev. A 71, 044301 (2005)
[19] Ai-Dong Zhu, Yan Xia, Qiu-Bo Fan, and Shou Zhang, Phys. Rev. A 73, 022338 (2006)
[20] C. H. Bennett, G. Brassard, and J. M. Robert, SIAM J. Comput. **17** 210 (1988).
[21] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. 76, 722 (1996).
[22] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A 54, 3824 (1996).
[23] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77** 2818 (1996).
[24] F. G. Deng and G. L. Long, Commun. Theor. Phys. **46** 443 (2006).

[25] N. Gershenfeld and I. L. Chuang, Science **275**, 350 (1997).

[26] D. G. Cory, A. F. Fahmy, and T. F. Havel, Proc. Natl. Acad. Sci. U.S.A. **94**, 1634 (1997); D.G. Cory, M. D. Price, and T. F. Havel, Physica D **120**, 82 (1998).

[27] R. Marx et al., Phys. Rev. A **62**, 012310 (2000).

[28] L. Xiao and G.L. Long, Phys. Rev. A **66**, 052320 (2002).

[29] D. X. Wei, X. D. Yang, J. Luo, X. P. Sun, X. Z. Zeng and M. L. Liu, Chin. Sci. Bull. **49**, 5423-426 (2004).

[30] W. Z. Liu, J. F. Zhang, Y. Cao, W. Y. Huo, L. Hao, G. L. Long, and Z. W. Deng, Appl. Phys. Lett. **94**, 064103 (2009).

[31] M. A. Nielsen, E. Knill, and R. Laflamme, Nature (London) **396**, 52 (1998).

[32] X. Fang, X. Zhu, M. Feng, X. Mao and F. Du, Phys. Rev. A **61**, 022307 (2000).

[33] J.F. Zhang, J. Y. Xie, C. Wang, Z. W. Deng, Z. H. Lu and G. L. Long, Sciences in China, G48, 706-715 (2005).

[34] V. Jacques, P. Neumann, J. Beck, M. Markham, D. Twitchen, J. Meijer, F. Kaiser, G. Balasubramanian, Phys. Rev. Lett. **102**, 057403 (2009).

[35] F. Casagrande, A. Lulli, and M. G. A. Paris, Phys. Rev. A **79**, 022307 (2009).

[36] S. Tanzilli, W. Tittel, M. Halder, O. Alibart, P. Baldi, N. Gisin and H. Zbinden, Nature, **437**, 116-120 (2005).

[37] H. Kosaka, H. Shigyou, Y. Mitsumori, Y. Rikitake, H. Imamura, T. Kutsuwa and K. Edamatsu, AIP Conference Proceedings **1110**, 245-248 (2009).

[38] G. L. Long, H. Y. Yan, and Y. Sun, J. Opt. B: Quantum Semiclassical Opt. **3**, 376 (2001).

[39] G. M. Leskowitz and L. J. Mueller, Phys. Rev. A **69**, 052302 (2004).